3713 Linden St
Bethlehem, PA 18020

October 18, 2021

Ms. Marlene H. Dortch
Secretary Federal Communications Commission
45 L Street NE
Washington, DC 20554

Reply Comment re: Docket No. 21-232 & No. 21-233, *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program.*

IPVM's initial comment presented the significant evidence that the covered entities, especially Hikvision and Dahua, pose a threat to the American public. Many of the more than 100 comments submitted in support of these entities failed to address, or outright dismissed, the real national security and cybersecurity concerns raised by the Commission. Many commenters instead focus on their own financial concerns and predict a collapse of America's surveillance camera supply and suppliers. We believe the FCC has a duty to place the security of the public above the interests of a select few. Still, we dispute that the side effects of these proposals will be as significant as many comments have claimed. Moreover, several comments made false or misleading statements, which we address here.

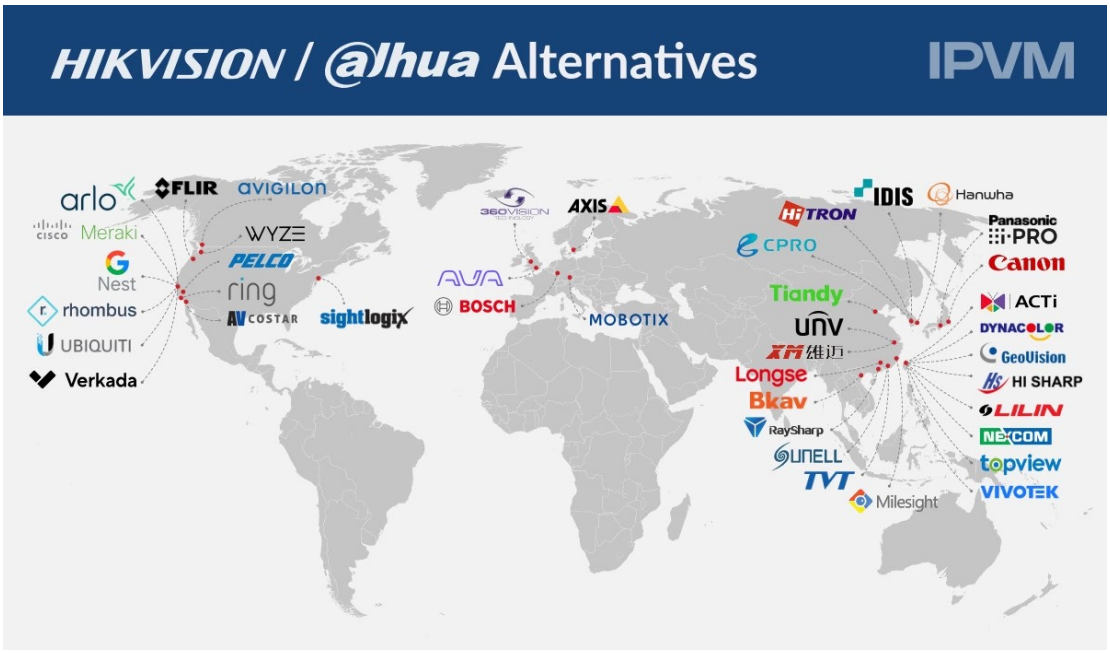
1. 40+ Options to Fill Hikvision & Dahua's Place

Numerous comments claimed the FCC's proposals will put American businesses in a position of being unable to source surveillance products. Our assessment is that the impacts will not be significant. The FCC's proposes to target only two surveillance manufacturers, albeit with significant market share; globally, numerous manufacturers exist that are capable of filling the gap, and the surveillance industry has already responded capably to disruptions effected by the NDAA ban.

A recent study published by IPVM identified more than 40 manufacturers globally - i.e. companies that develop their own firmware, software, and designs - that do serve as

alternatives to Hikvision and Dahua.[1] 13 of these manufacturers are based in the United States, while many others already sell in the United States (Figure 1).

Figure 1 - Hikvision/Dahua Alternatives



Others, in particular those based in Asia, have been unable to capture significant market share in the United States due to competition from Hikvision and Dahua. They may not be as widely known to many American businesses, but these manufacturers can easily fill the gap in the US market, and have even indicated a desire to do so. Uniview is China's 3rd largest surveillance company offering a range of products comparable in price and functionality to Hikvision and Dahua. Zhang Pengguo, the President of Uniview, is quoted in the Global Times describing the scrutiny on Hikvision and Dahua as "an opportunity for Uniview" who will "resolutely" seek to sell their products abroad.[2] Dahua own comment predicts that other manufacturers will step in, "Prohibiting two specific Chinese manufacturers from obtaining equipment authorization for video security products will not eliminate the demand for such products from U.S end users…the

---

[1] Ace, E. (2021, Aug 17). *40+ Alternatives to Dahua & Hikvision For Video Surveillance Camera Manufacturing*. IPVM. <https://ipvm.com/reports/hikvision-dahua-alternatives-directory?code=FCC>

[2] Cong, W. (2019, Mar 27). *China's Uniview undaunted by foreign political risks, takes Huawei case as rare lesson.* Global Times. <https://www.globaltimes.cn/content/1143676.shtml>

proposed rules will only create an incentive for other suppliers, including other Chinese companies, to enter the market to meet this demand."

Hikvision and Dahua's large-scale in the US has only been significant for the last 5 years. The market operated well before they entered, and will continue to operate after they exit. Comments significantly overstated the disruption and cost increases that may occur. American surveillance distributor ENS Security wrote that "other major manufacturers with comparable products range from five to fifteen times more expensive than Dahua Technology solutions." This claim is false. Not only are there comparable options in terms of products and price, even higher-end surveillance manufacturers do not approach price levels of "five to fifteen times more expensive than Dahua." In fact, ENS Security offers Uniview products with similar prices and capabilities to their Dahua offerings.

There is already some precedent for how American businesses might handle a forced switch away from Hikvision and Dahua, since the NDAA ban put much of the industry in this position. Since the ban, numerous US integrators and distributors have successfully switched to other suppliers with none of the catastrophic consequences predicted in comments. A large proportion of surveillance companies do business with the Federal government or with Federal contractors, making this is a fair litmus test. Moreover, even companies that do not do business with the Federal government have already taken this as a signal and moved away from Hikvision and Dahua.

2. Not Connecting to the Internet: A Band-Aid Solution

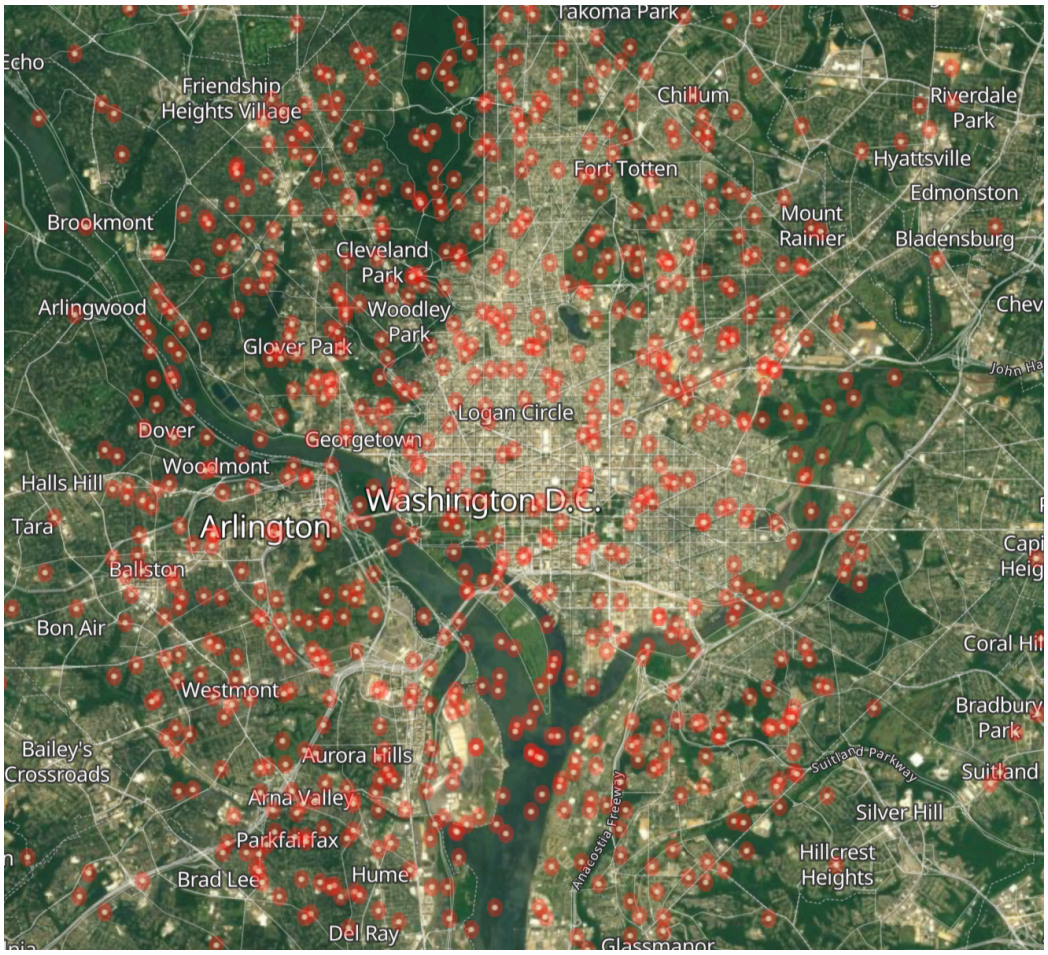
The vast majority of Hikvision and Dahua cameras fall into a category known as 'IP cameras', or 'Internet protocol cameras', a term the companies themselves use in marketing these devices. Hikvision, Dahua, and their supporters argue such equipment does not pose a risk because end users can voluntarily choose to not connect them to the internet. The Commission should be wary of this argument, which is specious to the point of actually being irrelevant. It is akin to suggesting laptops never connect to WiFi to ensure they can never be hacked; moreover, it is akin to a laptop manufacturer suggesting that because users may choose to not use WiFi, it does not matter that the laptops have vulnerabilities. The fact is these surveillance products are designed to be used with the Internet; Internet connectivity is a titular feature of Hikvision and Dahua's equipment, and this is increasingly what end users expect from surveillance products.

Nonetheless, both Hikvision and Dahua wrote at length about the possibility that their devices might not be connected to the internet in some deployments, and thus may not pose cyber risks of concern to the FCC. Hikvision said "As a practical matter, many

[cameras/recorders] are installed either on standalone internal networks that are not connected to the Internet at all" and that Hikvision equipment "operates within internal company systems that end users' IT departments design to be secure." Similarly, Dahua said "the vast majority of Dahua's equipment is not relevant to the Commission's concerns regarding national security risks to communications networks. For example, a significant amount of Dahua equipment imported, marketed, sold, and used in the United States is used in a closed network environment entirely disconnected from the broader public network such that prohibiting Dahua's equipment would not generate any increased security benefits to communications networks."

Internet-connected Hikvision and Dahua cameras are already common. Shodan, a search engine for internet-connected devices, has indexed nearly a million Hikvision and Dahua devices in the United States. Only publicly viewable devices connected to the Internet

Figure 2 - Hikvision Internet-Connected Devices in Washington D.C.
(Source: Shodan)



can be indexed by Shodan. By way of demonstration, Figure 2 shows Shodan-indexed Hikvision devices in the Washington D.C. area.

This number will only increase, consistent with consumer demands for internet-connected surveillance. It is unrealistic to rely on air gapping of these devices to address the FCC's cybersecurity concerns. Hikvision and Dahua design these devices to be used with the internet, and this how we should assume they will be used; it is unrealistic and dangerous to assume otherwise.

3. Entities Targeted Because They Are Chinese

Hikvision has claimed the FCC's proposals discriminate based on national origin, and claim this action is unconstitutional. Hikvision said "The Commission targets Hikvision and other companies…for only one reason: they are Chinese."

The FCC does not propose to target Chinese technology firms at large; being a Chinese company is not a sufficient condition to be on the covered entity list, and each of the five firms was selected for reasons that extend beyond national origin. These include being controlled or partially owned by the PRC state; ties to the People's Liberation Army; working with public security forces to design, supply and directly operate China's state mass surveillance, particularly in Xinjiang; cybersecurity concerns specific both to the companies' records and the high sensitivity of the data passing handled by their equipment; and other reasons, including any that may be classified.

Indeed, the PRC has used regulations over several years to disadvantage foreign technology firms under exactly the same rationale that the FCC uses for its proposals here. It has systematically bolstered domestic technology production while regulating against foreign manufacturers, arguing that these entities pose a cybersecurity risk. Xi Jinping has said "without cybersecurity, there can be no national security"[3], and his government promotes domestic technology production cybersecurity reasons. This mirrors the US government's concerns regarding Chinese technology, as well as actions taken by other governments. In August 2021, the Republic of China (Taiwan) announced a ban on all PRC-made technology products across its government, ordering them to removed by the end of 2021.[4]

---

[3] http://www.npc.gov.cn/zgrdw/npc/xinwen/2015-04/29/content_1934988.htm

[4] IPVM Team. (2021, Aug 17). *Taiwan Government Bans China Tech Including Dahua and Hikvision*. IPVM. <https://ipvm.com/reports/taiwan-gov-prc>

4. Hikvision False Claims

Hikvision's comment made multiple false or misleading claims.

Hikvision argues that "U.S. government officials and industry professionals agree that Hikvision equipment poses no national security threat…throughout this country [they] have acknowledged Hikvision's efforts in cybersecurity and dispelled any notions that Hikvision's video surveillance equipment poses a threat to the American telecommunications networks." As evidence, Hikvision misuses statements by two government officials while omitting many other statements to the contrary. First, they cite a 2018 statement by Army Colonel Christopher Beck that "We never believed [the cameras] were a security risk. They were always on a closed network." Hikvision says this means Col. Beck "firmly rejected the notion that the Army believed Hikvision cameras posed a security risk given their lack of internet connection." Again, it is unrealistic and dangerous to assume Hikvision products are not connected to the internet. Moreover, Col. Beck's statement is taken out of context. He was referring to surveillance used at a single Army base under his command. At no point did Col. Beck's take a position on Hikvision's potential security threats in a national context, neither was he expressing the Army's overall position on Hikvision's security threats. Furthermore, Col. Beck's comments were made before concerns with Hikvision were widely-known.

Since then, numerous US officials have said Hikvision is a security threat.

- In 2019 Randall Schriver, then the Asst. Secretary of Defense for Indo-Pacific Security Affairs, said "we're concerned given the nature of the relationship that these Chinese companies have with the CCP and the influence that the CCP may have on their decision-making and how they may be involved in state-sponsored goals such as theft of technology, intelligence, etc. So our first concern is the vulnerabilities that can be created by dealing with these companies."[5]
- Senator Tom Cotton described Hikvision and Dahua as "puppets of the Chinese Communist Party and the People's Liberation Army."[6]

---

[5] Honovich, J. & Rollet, C. (2019, Oct 16). *US DoD Comments on Huawei, Hikvision, Dahua Cyber Security Concerns*. IPVM. <https://ipvm.com/reports/schriver-jamestown>

[6] Rollet, C. (2019, Feb 7). *US Senator Calls Hikvision and Dahua "Puppets of the Chinese Communist Party", Urges Sanctions*. IPVM. <https://ipvm.com/reports/hikua-puppet>

- Katie Arrington, the CISO for DoD, said "we can no longer do business" with those using Hikvision.[7]
- In 2020, Hikvision was added to a list of "Communist Chinese Military Companies", a list of Chinese companies "owned or controlled" by the PRC military.[8]
- Since Col. Beck's comments, Congress passed the NDAA ban over national security/ cybersecurity concerns.

Hikvision cites a second official, Richard Driggers, Deputy Assistant Secretary for the DHS Office of Cybersecurity and Communications, for his comments that Hikvision patched a security vulnerability. Assistant Secretary Driggers states that when a Hikvision backdoor was discovered in 2017, "[W]e worked with [Hikvision]" and Hikvision "put out a software update that mitigated the impacts of this particular exploitation . . . [a] standard practice that we do at the Department of Homeland Security across many different companies' devices and software." This is far from evidence that "U.S. government officials and industry professionals agree that Hikvision equipment poses no national security threat." Instead, he describes Hikvision doing nothing more than what is expected of any company when a vulnerability is found; as Asst. Sec. Driggers said, this is a "standard practice that we do at the Department of Homeland Security across many different companies[.]" It is important to note that this vulnerability was a backdoor; *by definition, Hikvision themselves created the 2017 vulnerability in the first place.*

Hikvision explains that two of the services they operate, HikConnect and HikCentral, do require an internet connection but claim to have no visibility into user data. Fundamentally, this is untrue because all service providers, by definition, have access to the service they provide. Any cloud provider has a level of visibility; in Hikvision's case, this would include the IP addresses and corresponding geocodes of the hundreds of thousands or millions of US devices connected to these services.

Hikvision says says they have "a stellar record of identifying and addressing security vulnerabilities in a transparent manner." They further state that "No purpose is served by singling out Hikvision cameras and equipment for treatment different from that afforded other equipment—whether security equipment or other networkable devices—with equivalent or greater vulnerabilities…Hikvision equipment does not raise any security

---

[7] Rollet, C. (2020, Apr 8). *US DoD Declares "Can No Longer Do Business" With Contractors Using Dahua, Hikvision, Huawei*. IPVM. <https://ipvm.com/reports/dod>

[8] Rollet, C. (2020, Jun 26). *Hikvision Put on US DoD "Communist Chinese Military Companies" List, Faces Risk of Presidential Sanctions.* IPVM. <https://ipvm.com/reports/us-dod-ccp-list>

issue distinct from those posed by a myriad of other networkable devices." It should be noted that Hikvision touts its transparency in the very same comment that was corrected after failing to disclose a critical vulnerability discovered last month. That aside, Hikvision's record is far from "stellar." Not only do Hikvision and Dahua frequently have cybersecurity incidents, these incidents tend to involve critical vulnerabilities rather than minor cybersecurity lapses. Hikvision does not explain their methods in assessing that other manufacturers have had "equivalent or greater vulnerabilities", nor do they provide any supporting evidence. Even taking this for granted, other surveillance companies with "equivalent or greater vulnerabilities" are not tied to the PRC state, an essential feature of the risks posed by Hikvision and Dahua.

Hikvision has also directly encouraged port forwarding, a practice that exposes devices to hacking. Hikvision acknowledged in their comment that port forwarding is a dangerous practice. Yet, Hikvision's cybersecurity best practices page continue to recommend port forwarding for users that want "quick and steady" remote access to Hikvision devices.[9]

Hikvision also argues that, "A scheme that entirely bars a Chinese manufacturer from the U.S. market while imposing no restrictions on companies from Russia, Iran, or North Korea is not narrowly tailored." There are no video surveillance manufacturers in Iran or North Korea. It should be noted that there are no comparable surveillance manufacturers in Russia, Iran, or North Korea. China is the largest exporter surveillance, and home to the industry's largest companies, such as Hikvision.

5. Dahua False Claims

Dahua also makes false statements and misrepresentations in their comment.

Dahua claims, "the Commission has not made any particularized finding that Dahua as a company, or any of the equipment that it manufactures, poses a threat to U.S. national security." This is clearly false. In March 2021, the FCC deemed Dahua a national security threat, and several FCC Commissioners reiterated this position at the June meeting.

Dahua states that, "Only a miniscule portion of Dahua Technology's ownership (via shares held on the Shenzhen Stock Exchange) is indirectly (through state-owned enterprises) attributable to the government of the People's Republic of China or other

---

[9] Honovich, J. (2021, Sep 20) *Hikvision Has "Highest Level of Critical Vulnerability," Impacting 100+ Million Devices*. IPVM. <https://ipvm.com/reports/hikvision-36260>

government entities." The "minuscule portion" of PRC government ownership is more than 10%, which more reasonable people would not describe as "miniscule."

Dahua also claims "there is no evidence that any named vendor (including Dahua) has violated any of the existing criteria or rules governing equipment authorizations." This is true to the best of our knowledge. However, it is worth noting that the South Korean Ministry of Science and ICT - which enforces rules similar to those enforced by the FCC - recently revoked 21 of Dahua's product authorizations over forged test reports, while 224 Hikvision authorizations were revoked.[10]

6. Hytera False Claims - No Ties to Chinese Communist Party

Hytera (HCC) said in their comment that "HCC is not owned or controlled by, or otherwise affiliated with, the Chinese government; it is not owned or controlled by any entity affiliated with the Chinese defense industrial base. HCC has no ties to the Chinese Communist Party." HCC has already submitted an additional comment acknowledging that a PRC state investment firm is slated to purchase a 10% stake of the company.

Figure 3 - Hytera Employees Taking Party Oath

[10] Patton, S. (2020, Dec 10). *Hikvision, Dahua, and Uniview Falsify Test Reports To South Korea*. IPVM. <https://ipvm.com/reports/hikuaview-sk>

Beyond this, our research found substantial evidence of ties to the Chinese Communist Party.

HCC supports Chinese Communist Party committees across its organization. The company runs a very active WeChat account (hosted directly by Hytera) called the "Hytera Party Member Vanguard" which notes "The party committee of Hytera was established in December 2005, and always adheres to the leadership of the CPC." The account features posts in which Hytera employees travelled to Shaoshan, Mao Zedong's hometown to "carry out research activities" and "commemorate the great achievements of Chairman Mao Zedong." A recent post (Figure 3) shows multiple employees taking the oath to join the CCP, with a Hytera sign in the background.

In May, Hytera even won an award from Guangdong Province for its Communist Party organizing success, which cites "Hytera's efforts to do a good job in party building over the years." Li Xin, a Hytera VP who was the company's party secretary, once said, "Our company has always established a party building philosophy, which is to be with the party and communicate its needs." HCC's claim of "no ties to the Chinese Communist Party" cannot be reconciled with the significant evidence of support for the Chinese Communist Party within their own organization.

7. Conclusion

The comments on this action downplay, mislead, or altogether ignore the serious cybersecurity and national security issues at play. Both Hikvision and Dahua had critical vulnerabilities disclosed during the comments period, a fact that neither the companies nor their partners addressed in comments. Rather than addressing these issues, comments from various businesses and industry associations focus on their own financial interests while overstating the impact of the FCC's proposals; additionally, many comments made false or misleading claims. We urge the FCC to stick to the facts and represent the best interests of the public as it proceeds with this action.

Sincerely,

John Honovich
President, IPVM
john@ipvm.com

Conor Healy
Government Director, IPVM
chealy@ipvm.com